International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 6, Nov-Dec 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Building Data Compliance Management System

Liu Guangpu, Bi Guoyi, Yang Wenhao, Ma Ping

School of Law, Beijing Wuzi University, Beijing, China

ABSTRACT

With the vigorous development of strong artificial intelligence, China plays an increasingly important role in the development of generative artificial intelligence. However, due to the inherent lag of the law itself, as well as the competition of various artificial intelligence developers to catch up, resulting in many data compliance issues during the development process of artificial intelligence. Therefore, this paper proposes to set up a data compliance management system to solve the data compliance risks that may be involved in the generation stage of artificial intelligence, to achieve data compliance by managing manual trainers during the processes of data generation, communication, and application. We expect these solutions to promote the continued healthy development of AI compliance and contribute to the improvement of AI-related legislation.

KEYWORDS: *data compliance, network security, legal risk*

How to cite this paper: Liu Guangpu | Bi Guoyi | Yang Wenhao | Ma Ping "Building Data Compliance Management System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-6, December 2024, pp.339-351, URL: www.ijtsrd.com/papers/ijtsrd71578.pdf

IJTSRD71578

I. Foreword

In the current stage of artificial intelligence development, data compliance has become a major problem in various areas. The main reasons for these 1 dilemmas include both external and internal reasons. The external reason is the emergence of artificial intelligence as a new entity, coupled with the lag of the law itself; the current legal system cannot fully encompass it, such as personal information protection laws and copyright laws, which, along with other relevant regulations, still need to be updated and improved. The internal reason is that the development of artificial intelligence is based on a large number of databases, so most artificial intelligence development companies use non-compliant means such as web crawlers to obtain data in order to seek large amounts of high-quality data, in order to develop artificial intelligence.

This practice will create a series of potential risks. Although the data feeding is carried out within the company and has the characteristics of concealment, it leaves hidden risks. Therefore, we try to build a compliance management system, which integrates the basic structure of the organization, implementation policies, data processing processes and compliance audit procedures to achieve the expected compliance results, and take corresponding actions to prevent, detect and respond to non-compliant data processing behaviors, which need to be continuously maintained and improved.

Based on current relevant laws and regulations, the organization also considers relevant foreign legislation and the development prospects of artificial intelligence, envisioning the formulation of relevant domestic laws in the future. This approach guides the organization in building a compliance management system to direct future data processing, risk handling, and compliance reviews for all employees, including leadership. The following are the specific steps to build a compliance management system.

II. Data Guide

The organization first establishes and maintains independent documentation, which the author named the data guide. The data guide is divided into 3 parts, which include national mandatory regulations, relevant foreign regulations for reference, and rules specially designed by the organization for the establishment of the compliance management system.

A. National Mandatory Provisions

Licenses, licenses or other forms of authorization by national laws and regulations; Orders, rules or guidelines issued by regulatory bodies; Decisions of courts or administrative tribunals. These are constitutional provisions that must be observed by all members of the organization and cannot be changed or revoked. The following are some specific relevant legal provisions:

Cybersecurity Law

The construction and operation of the network or the provision of services through the network shall, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, take technical measures and other necessary measures to ensure the security and stable operation of the network, effectively deal with network security incidents, prevent network illegal and criminal activities, and maintain the integrity, confidentiality and availability of network data.

Network operators shall, in accordance with the requirements of the network security level protection system, take technical measures to monitor and record the network operation status and network security events, and keep relevant network logs for not less than six months in accordance with the provisions.

Network operators shall formulate emergency plans for network security incidents, and promptly deal with security risks such as system vulnerabilities, computer viruses, network attacks, and network intrusions; when incidents that endanger network security occur, immediately initiate emergency plans, take corresponding remedial measures, and follow regulations Report to relevant competent authorities.

Network operators shall take technical measures and other necessary measures to ensure the security of the personal information they collect and prevent the information from being leaked, damaged or lost. In the event of leakage, damage, or loss of personal information, remedial measures shall be taken immediately, and users shall be notified in a timely manner in accordance with regulations and reported to the relevant competent authorities.

The operation of critical information infrastructure shall formulate emergency plans for network security incidents and conduct regular drills.

If the relevant departments of the people's government at or above the provincial level, in performing their duties of network security supervision and management, find that there are greater security risks or security incidents in the network, they may interview the legal representative or principal responsible person of the operator of the network in accordance with the prescribed authority and procedures. Network operators shall take measures to rectify and eliminate hidden dangers in accordance with the requirements.

If an emergency or production safety accident occurs due to a network security incident, it shall be handled in accordance with the "the People's Republic of China Emergency Response Law", "the People's Republic of China Safety Production Law" and other relevant laws and administrative regulations.

The national definition of data outbound: network operators provide personal information and important data collected and generated during their operations in the People's Republic of China through the Internet and other methods to overseas institutions through direct provision or development of business, provision of services, products, etc. One-time activities or continuous activities of organizations or individuals.

The specific circumstances include the following: 1. Provide personal information and important data to subjects within the territory of the country, but not within the jurisdiction of the country or not registered in the territory. 2. The data has not been transferred and stored outside the country, but has been accessed and viewed by institutions, organizations and individuals outside the country (except for public information and web page access). 3. The internal data of the network operator group is transferred from domestic to overseas, involving personal information and important data collected and generated in its domestic operations.

The circumstances that do not belong to data exit include: personal information and important data collected and generated in non-domestic operations that exit through the country without any change or processing, do not belong to data exit.

Personal information and important data collected and generated in non-domestic operations are stored and processed in the country and then left the country, and personal information and important data collected and generated in domestic operations are not considered as data exit[1].

In addition, the compliance path for China's data exit and the new SCC regulations for Guangdong, Hong Kong and Macao Bay Area have the following provisions:

The "Personal Information Exit Standard Contract Measures" issued on February 22, 2023 clearly defines the scope of supervision: domestic personal information processors export personal information to

overseas recipients. The filing authority is the provincial network information department where it is located. The filing materials provided are: 1 standard contract. 2 Personal Information Protection Impact Assessment (PIA) report. 3 procedural materials, including procedural materials including a. unified social credit code documents, legal representative identity documents and photocopies of the identity documents of the handling person B. power of attorney of the handling person c. letter of commitment.

The scope of supervision in the "Guidelines for the Implementation of Standard Contracts for the Cross-border Flow of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)" issued on December 10, 2023 is: 1 Mainland personal information processors in the Greater Bay Area to receive outbound personal information from Hong Kong. information. 2. The personal information processor in Hong Kong transmits personal information to the mainland recipient in the Greater Bay Area.

The security authorities shall be: the Internet Information Office of Guangdong Province, or the Office of the Government Information Technology Director of the Government of the Hong Kong Special Administrative Region. The required filing materials are: 1. Standard contract 2. Procedural materials: a. of photocopies of the identity documents of the legal representative. B, letter of commitment.

Provisions on reporting and notification obligations:

Network operators shall formulate emergency plans for network security incidents and deal with security risks such as system loopholes, computer viruses, network attacks and network intrusions in a timely manner; in the event of an incident endangering network security, immediately start the emergency plan, take corresponding remedial measures, and report to the relevant competent departments [1]in accordance with the provisions.

In the event of disclosure, tampering or loss of personal information occurring or likely to occur under the Personal Information Protection Law, the personal information processor shall immediately take remedial measures and notify the departments and individuals [2]performing the duties of personal information protection.

The Data Security Law shall strengthen risk monitoring in data processing activities, and immediately take remedial measures when data security defects, loopholes and other risks are found; when data security incidents occur, they shall immediately take measures to deal with them, inform users in time and report [3]to the relevant competent departments in accordance with the provisions.

"Emergency Plan for Public Internet Network Security Emergencies" Basic telecommunications companies, domain name agencies, and Internet companies shall closely monitor the operation of their own networks and systems. In the event of a network security emergency specified in this plan, they shall immediately pass the telephone. Report to the Ministry's Emergency Office and the relevant provincial (autonomous region, municipality) communications administrations in other ways, and shall not report late, falsely, conceal, or omission. Network security professional institutions and network security enterprises shall monitor and collect information on public Internet network security emergencies that have occurred through various channels, and report to the Ministry's Emergency Office and the relevant provincial (autonomous region, municipality directly under the Central Government) Communications Administration in a timely manner. When reporting emergency information, it shall state the time of occurrence of the incident, the scope of influence and harm preliminarily determined, the emergency measures taken and relevant suggestions.

Special Emergency Plan for Network and Information Security Incidents in Shanghai (2014 Edition)

Information Report

Units that have network and information security incidents must report orally within half an hour and in writing within one hour to the duty room of the municipal network security office (located in the municipal network and information security emergency management affairs center, on duty telephone number: 021-22816787), the municipal emergency linkage center and the county government of the incident area. Major network and information security incidents or special circumstances must be reported immediately.

In the event of a major network and information security incident, the Municipal Network Security Office and the Municipal Emergency Linkage Center must report to the Municipal Party Committee General Duty Office and the Municipal Government General Duty Office orally within 1 hour and in writing within 2 hours after receiving the report; extra-large network and information security Incidents or special circumstances must be reported immediately.

Measures for the Administration of Cybersecurity Incident Reports (Draft for Comments)

In the event of a network security incident, the operator shall promptly start the emergency plan for disposal. According to the network security incident classification guidelines, belong to the larger, major or particularly significant network security incidents, should be reported within 1 hour.

If the network and system belong to the various departments of the central and state organs and the enterprises and institutions under their management, the operator shall report to the network information work organization of the department. Belonging to major, particularly significant network security incidents, the departments of the network letter work agencies in the receipt of the report should be reported to the national network letter department within 1 hour.

Where networks and systems are critical information infrastructure, the operator shall report to the protection work department and the public security organ. Belonging to major, particularly major cyber security incidents, the protection work department shall, after receiving the report, report to the State Internet information department and the public security department of the State Council within one hour.

Other network and system operators shall report to the local network information department. Belonging to major, particularly major network security incidents, the territorial network information department after receiving the report, should be within 1 hour to the higher level of network information department report.

If there is a competent regulatory department of the industry, the operator shall also report in accordance with the requirements of the competent regulatory department of the industry. If a suspected crime is found, the operator shall report to the public security organ at the same time.

Network Data Security Management Regulations (Draft)

In the event of a data security incident such as leakage, damage, or loss of important data or personal information of more than 100,000 people, the data processor shall also perform the following obligations:

(1) report the basic information of the incident to the district-level network information department and relevant competent authorities within eight hours of the occurrence of a security incident, including the amount of data involved, type, possible impact, and disposal measures that have been or are to be taken;

The (2) shall report the investigation and evaluation report including the cause of the incident, hazard consequences, responsibility handling, improvement measures, etc. to the districted municipal network information department and relevant competent departments within 5 working days after the incident is handled.

Regarding the classification of events and the judgment of the degree of harm, there are also specific provisions in my country's "Measures for the Management of Cyber Security Incident Reports (Draft for Comment):

Particularly significant data security incidents:

1. Important data is leaked or stolen, posing a particularly serious threat to national security and social stability.
2. disclosure of personal information of more than 0.1 billion people.
3. The network platform has been attacked and tampered with, resulting in the spread of illegal and harmful information. One of the following situations can be regarded as "extra-large scope":
   a. appears on the homepage and lasts for more than 6 hours, or appears on other pages and lasts for more than 24 hours;
   b. Forward it more than 100000 times through social platforms;
   c. More than 1 million times of browsing or clicking;
   d. above the provincial level network information departments, public security departments identified as "large-scale communication.
4. Cause direct economic losses of more than 0.1 billion yuan,
5. Other data security incidents that pose a particularly serious threat to national security, social order, economic construction and public interests and have a particularly serious impact.

Significant data security incidents:

1. important data leakage or theft, pose a serious threat to national security and social stability.
2. disclosure of personal information of more than 10 million people,
3. The network platform has been attacked and tampered with, resulting in the wide spread of illegal and harmful information. One of the following situations may be considered as "extensive":
   a. appears on the homepage and lasts for more than 2 hours, or appears on other pages and lasts for more than 12 hours;

b. Forward it more than 10000 times through social platforms;
c. More than 100000 times of browsing or clicking;
d. above the provincial level network information departments, public security departments identified as "large-scale dissemination.

4. caused direct economic losses of more than 20 million yuan.

5. Other data security incidents that pose a serious threat to national security, social order, economic construction and public interests and have a serious impact.

Larger data security events:

1. important data leakage or theft, pose a serious threat to national security and social stability.

2. disclosure of personal information of more than 1 million people.

3. The network platform has been attacked and tampered with, resulting in the spread of illegal and harmful information on a large scale. One of the following situations may be considered as "larger scope":

a. appears on the homepage and lasts for more than 30 minutes, or appears on other pages and lasts for more than 2 hours;
b. Forward it more than 1000 times through social platforms;
c. More than 10000 times of browsing or clicking;
d. above the provincial level network information departments, public security departments identified as "large-scale dissemination.

4. caused direct economic losses of more than 5 million yuan.

5. Other data security incidents that pose a serious threat to national security, social order, economic construction and public interests and have a serious impact.

General data security events:

In addition to the above-mentioned data security incidents, data security incidents that pose a certain threat to national security, social order, economic construction and public interests and have a certain impact.

What the report needs to include:

Measures for the Administration of Cybersecurity Incident Reports (Draft for Comments)

The operator shall report the incident in accordance with the Cybersecurity Incident Information Report Form, including at least the following:

(1) the name of the unit where the incident occurred and the basic information of the facilities, systems and platforms where the incident occurred;

(2) the time, place, type, impact and harm of the event, measures and effects. For ransomware attacks, the amount, method, date, etc. of the ransom should also be included.

Trends in (3) developments and possible further impacts and hazards

(4) preliminary analysis of the cause of the incident;

(5) clues required for further investigation and analysis, including information on possible attackers, attack paths, existing gushing holes, etc;

(6) further response measures to be taken and matters requiring support;

Protection of (7) incident site;

(8) other information that should be reported.

After the incident is handled, the operator shall conduct a comprehensive analysis and summary of the cause of the incident, emergency response measures, hazards, responsibility handling, rectification, lessons, etc. within 5 working days, and form a report to be reported in accordance with the original channel.

B. Relevant foreign laws and regulations

Organizations can refer to the relevant EU regulations:

EU: GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The General Data Protection Regulation ("GDPR"), which is generally applied by the EU for the protection of personal data, stipulates that "personal data may not be transferred to a country or region outside the EU unless that country or region ensures a level of protection equivalent to that of the EU for the rights and freedoms of the data subject in relation to the processing of personal data. Personal data can be legally transferred across borders in the following three circumstances:

1. transfer to a country or territory with an equivalent level of protection as determined by the EU;

2. transfer to a country or region that provides appropriate safeguards to ensure adequate data protection;

3. Or transfer on the basis of exemption.

The protection of non-personal data outside the EU is often invoked under the Data Act.

The protection of non-personal data in the EU usually invokes: Regulation on the free flow of non-personal data

The relevant laws of the European Union stipulate that when the destination of the data leaving the country has not been fully determined by the European Union, the data controller or processor can only provide appropriate safeguards and meet the conditions that the data subject can exercise its rights and obtain effective legal remedies. Subject within the EU can transfer [4]the relevant personal data to a third country or international organization.

Article 46 of the GDPR also provides for a number of appropriate safeguards:

1. Legality-binding and enforceable instruments between public authorities
2. BINDING COMPANY RULES (Binding Corporate Rules, BCRs)
3. Standard contractual clauses adopted or approved by the European Commission (Standard Contractual Clauses, SCCs)
4. Approved Code of Conduct (Codes of conduct)
5. Approved certification mechanisms (certification mechanism)

In addition, the cross-border path of personal data in the EU has the following provisions for specific exemptions: in the case of adequacy determination and appropriate safeguards can not be met, the cross-border demand side of the data can also retreat to determine whether the cross-border transmission of its data is exempt under specific circumstances.

Article 49 of the GDPR enumerates cases of exceptions to exemptions that have not been recognized and have not reached binding rules, which can be divided into three categories:

1. The data subject agrees, I .e. the data subject is clearly informed of the risk but still agrees to transfer;
2. A series of necessary circumstances, including: necessary to fulfill the requirements of the contract, necessary in the public interest, necessary to exercise legal rights, necessary to protect the interests of the data subject (subject to the premise that the data subject is unable to express consent due to special reasons);
3. According to a legitimate purpose, such as data transfer is to provide consultation to a person with a legitimate interest.

US: (for public companies) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (effective 2023.9.5)

The new rules will require registrants to disclose on the new ltem 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant. An Item 1.05 Form 8-K will generally be due four business days after a registrant determines that a cybersecurity incident is material. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing The new rules also add Regulation S-K Item 106, which will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. Item 106 will also require registrants to describe the board of directors' oversight of risks from cybersecurity threats and management' s role and expertise in assessing and managing material risks from cybersecurity threats. These disclosures will be required in a registrant's annual report on Form 10-K. [5]

S. domestic issuers disclose significant cybersecurity incidents by completing Form 8-K and cybersecurity risk management, strategy and governance by completing Form 10-K annually.

The rules require comparable disclosures by foreign private issuers on Form 6-K for material cybersecurity incidents and on Form 20-F for cybersecurity risk management, strategy, and governance.

Foreign private issuers should use Form 6-K to disclose relevant significant cybersecurity incidents and Form 20-F to disclose cybersecurity risk management, strategy and governance.

The United States has also established a number of trade agreements on cross-border data, such as the U. S.-Korea Free Trade Agreement, the Trans-Pacific Partnership Agreement ("TPP") and the U. S.-Mexico-Canada Trade Agreement ("USMCA"). Facilitate the removal of data localization and promote cross-border data liberalization. At the same time, bilateral agreements will be established: the EU-US Data Privacy Framework ("DPF"), the UK-US Data Access Agreement, the Australia-US Cloud Act Agreement and OECD rules: APEC Data Cross-

border Flow Privacy Framework, Cross-border Privacy Rules ("CBPR") to facilitate law enforcement agencies to access cross-border data and voluntary certification by enterprises, after passing, personal information can be exchanged freely within the certification system.

In the United States, many regulations and bills have been set up to restrict the export of data in key technologies and specific fields, define the "scope of sensitive data", expand the extraterritorial application of domestic law through "long-arm jurisdiction", and other subdivision rules for sub-sector and sub-industry supervision. For example: Export Control Regulations ("EAR"), Foreign Investment Risk Assessment Modernization Act ("FIRRMA"), Chip Semiconductor: New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to China, Advanced Computing Chip Rules, Interim Final Rules on Export Control of Semiconductor Manufacturing Items, "Controlled Non-Secret Information List" ("CUI"),(Clarification of Foreign Lawful Use of Data Act ("CLOUD Act"),(Public Company Cybersecurity Risk Management, Policy, Governance and Event Disclosure Rules "," Financial Services Modernization Act "," Children's Online Privacy Protection Act "," Cybersecurity Information Sharing Act "," California Consumer Privacy Protection Act ", etc.

C. Organization internal rules and regulations

In order to strengthen data compliance and facilitate management, the organization specially formulates relevant articles of association after referring to relevant legal documents, predicting the future direction of legal norms and investigating the market data processing situation, which are also the articles of association that the organization must abide.

Judging of event classification and hazard degree: Threat indicators are traces or evidence of intrusion or malicious activity found in a system or network. These metrics help identify potential security threats, such as malware infections, data breaches, or unauthorized access.

Security experts can assess the impact of security events based on factors such as the type of IOC, the systems involved in the IOC, data, network segments, and active time. Often, multiple different types of IOCs are present at the same time, meaning that a larger range of intrusions may be suffered.

Specific IOC types have abnormal network traffic, and the network traffic pattern of entering and leaving the organization has changed. Changes in system configuration, enabling remote access, or disabling security software. Abnormal login signals, logins at unusual times or in unusual geographic locations, repeated failed login attempts. Unusual file access requests, multiple requests for a single file, or attempts to access through multiple means. and DNS request exception.

III. Compliance management system planning

The establishment of a compliance management system requires departmental planning. The purpose of planning is to predict possible situations and consequences; it is preventive in nature. Based on the results of the compliance risk assessment, the organization needs to plan how to address adverse effects before they occur and how to benefit from the enabling conditions or environment that contribute to the compliance management system. Planning also needs to determine how actions deemed necessary or beneficial to the compliance management system are incorporated into pre-training and procedures. Other systems for assessing the effectiveness of the compliance management system should also be planned, which may include monitoring, measurement techniques, internal audits or management reviews.

The purpose of the compliance management system is to pre-train the compliance of processing data, and the organization needs to use control means to achieve these 1 purposes. The organization implements control tools that include clear, practical, and easy-to-follow documented operational policies, processes, procedures, and data guidelines, as well as corresponding investigation procedures.

A. Guidelines for Data Compliance Management Systems

The Organization has well-functioning mechanisms in place to investigate, in a proper and thorough manner, any allegations or suspicions of misconduct against the Organization, its personnel or related third parties. This includes the organization's response documentation, any disciplinary or remedial action taken, and any revision of the compliance management system following lessons learned. The investigative mechanisms developed by the Organization require the identification of the root causes of misconduct, including by managers, top management and governance bodies, gaps in the compliance management system and the reasons for the lack of accountability. A rigorous root cause analysis involves the number and level of personnel, as well as the degree, prevalence, severity, duration and frequency of non-compliance. The investigation pursued by the organization is impartial and independent. An independent committee shall be established to supervise the investigation and ensure the integrity and independence of the investigation.

The organization establishes an investigation and reporting mechanism with reference to relevant domestic and foreign laws on reporting notification obligations, and sets the level of reporting investigation results with reference to national regulations. Even if the law does not require organizations to report non-compliance, organizations may consider proactively disclosing non-compliance to regulators to mitigate the consequences of non-compliance.

Data protection authorities collect information in a variety of ways. Taking into account the size, scope, nature and complexity of the organization, the organization adopts the following methods of information collection: ad hoc reports of detected or identified non-compliance; information obtained through hotlines, complaints and other feedback channels (including tip-offs); informal discussions, seminars and focus groups; sampling and integrity testing, such as mystery customers; cognitive findings; direct observation, formal interviews, facility visits and inspections; audit and review; Interested party inquiries, training requirements and feedback provided during training (especially personnel).

B. performance evaluation system

In order to determine the compliance of data processing in the pre-training phase, the organization requires that the processing data need to be monitored. Monitoring is the process of gathering information to assess the effectiveness of the compliance management system and the compliance performance of the organization. The data information obtained from the monitoring is used to evaluate the degree of data compliance and system perfection in the pre-training phase. These 1 tasks are performed by the data protection department established by the organization.

The effectiveness of the conduct examined by the Organization typically includes: the effectiveness of training; the effectiveness of controls; the effective allocation of responsibility for meeting compliance obligations; the timeliness of compliance obligations; the effectiveness of addressing previously identified compliance deficiencies; the failure to conduct internal compliance checks as planned; and the review of business strategies for compliance risks for appropriate updates. Non-compliance and risk-taking (e. g., events that do not have a negative impact); non-fulfilment of compliance obligations; non-achievement of objectives; current status of compliance culture; establishment of leading and lagging indicators.

Sources of feedback on the organization's compliance performance are generally through whistle-blowing facilities, helplines, situation feedback, suggestion boxes, key customers, e.g., through complaint handling systems, and third parties, e.g., data providers, regulators. Or through process control logs and activity records (including computer and paper records).

C. Classification, storage and information retrieval systems

The organization establishes an information management system to capture issues and complaints, and to classify and analyze compliance-related issues and complaints. Analyze and consider the systemic and repetitive nature of issues in order to correct or improve issues that are more difficult to identify and may pose significant compliance risks to the organization.

The Organization's criteria for classifying information are mainly the following indicators: source; sector; description of non-compliance issues; reference to obligations; severity; and actual and potential impact.

D. Development of indicators

The risk crisis predicted by the compliance management system needs to be systematically analyzed on the basis of certain data indicators. The 1 process of developing indicators should take into account the results of the compliance risk assessment to ensure that the indicators are relevant to the organization's compliance risk characteristics. While the question of how to measure compliance performance may remain challenging in some respects, the Organization considers it to be an important part of demonstrating the effectiveness of the compliance management system. In addition, the required indicators will change with the maturity of the organization and the timing and extent of the implementation of new and revised programmes. The indicators thus identified include the following: the proportion of effective trainers; the frequency of regulatory intervention; and the extent to which the feedback mechanism is used (including the evaluation of the mechanism by users). Reactivity indicators may include: non-compliance issues identified, reported by type, area and frequency; consequences of non-compliance, including an assessment of the impact on monetary compensation, fines and other penalties, remediation costs, reputation or personnel time costs; and time spent reporting and taking corrective actions. Non-compliance trend (expected compliance rate based on past trends).

E. Compliance Report

While it is important to report systemic and repetitive issues, it is equally important to focus on a major or

intentional non-compliance. Minor issues may also indicate serious deficiencies in current processes and compliance management systems. If not reported in a timely manner, it may cause the problem to be ignored and may cause such failures to become systemic problems. The so-called compliance report should specifically include: any matters that the organization needs to notify the regulatory agency; Changes in compliance obligations, their impact on the organization, and proposed actions to meet new obligations; Measurement of compliance performance, including non-compliance and continuous improvement; The number and details of possible non-conformities, and subsequent analysis; Corrective actions taken; Information on the effectiveness, achievements and trends of the compliance management system; the development of contacts and relationships with regulatory bodies; The results of audit and monitoring activities; The complete implementation of monitoring action plans, especially based on audit reports or regulatory requirements, or both.

F. Record keeping

Record keeping should include the recording and classification of compliance and suspected non-compliance issues during the pre-training phase, as well as actions taken to resolve the issues. Records shall be stored in such a way as to ensure clarity and ease of identification and retrieval. Records shall be protected against any addition, deletion, modification, unauthorized use or concealment.

The organization's compliance management system records include: compliance performance information, including compliance reports; details of non-compliance and corrective actions; compliance management system review and audit results, and actions taken.

G. System update

The effectiveness of a compliance management system is characterized by its capacity for continuous improvement and development. As the organization's internal and external environment and operations change over time, so do the nature of its customers and the applicable compliance obligations. Therefore, we set up a data protection committee to be responsible for the updating of documents and the improvement of the system.

The adequacy and effectiveness of the compliance management system is assessed by the Data Protection Board on an ongoing and regular basis using a variety of methods, such as analysis using the results of reviews conducted by data protection authorities. The Data Protection Board shall establish measures to review its compliance management system and ensure that it is up-to-date and appropriate for its objectives. In determining the scope and time scale of action to support continuous improvement, the Committee should take into account the historical context, economic factors, and the effects of pre-training and other relevant circumstances. A survey of organizational personnel can also be conducted to gauge the compliance culture and assess the strength of controls. Further sources of information for continuous improvement may be the results of user surveys, reports of concern, periodic monitoring, audits, or management reviews.

The organization shall consider the results and outputs of such assessments to determine whether there is a need or opportunity for changes to the compliance management system. In order to help ensure the integrity and effectiveness of the compliance management system, changes in each element of the management system should take into account its dependence on and impact on the effectiveness of the overall management system. When making changes to the compliance management system, the organization shall consider the impact of these changes on the compliance management system, the organization's operations, resource availability, compliance risk assessment, the organization's compliance obligations and its continuous improvement process.

H. nonconformity and corrective action

The failure of a data protection department to prevent or detect one-off non-compliance does not necessarily mean that the compliance management system lacks effectiveness in preventing and detecting non-compliance incidents. It may only be due to the current non-compliance issues that are not showing up. It is more important to re-evaluate product and service performance when analyzing non-conforming or non-compliant information. Where non-compliance is significant, consider changing organizational practices and procedures; retraining personnel; reassessing the need to notify stakeholders; providing early warning of potential non-compliance issues; redesigning or reviewing controls; strengthening notification and communication procedures (internal and external); and communicating facts about non-compliance and the organization's position on non-compliance. The organization should determine the root causes of non-compliance with the policy or procedures, or both, and update the policy and procedures based on lessons learned.

IV. Establishment of a Data Protection Department, Data Protection Commission

Following the establishment of the compliance management system, a dedicated compliance management department must be established for supervision and management. The establishment of a compliance management department requires strong support from top management. To ensure that compliance management systems are effective, governance bodies and top management need to lead by example by adhering to and actively and explicitly supporting compliance and compliance management systems. Top management should encourage the creation and support of compliance behavior, and should not tolerate violations of compliance behavior. In order to enable the compliance management department to effectively fulfill its management and supervision responsibilities, rather than a superficial department. Top management should ensure that: the organization's commitment to compliance values, goals and strategies is aligned to properly position compliance; all personnel are encouraged to recognize the importance of achieving their responsible compliance goals; 1 is an environment that encourages reporting of violations and that those who report violations are not subject to retaliation; Compliance is integrated into the broader organizational culture and culture reform approach; identify non-compliant content and take immediate action to correct or resolve it; operating targets and metrics do not affect compliance behavior. In addition, top management should refer to KPIs and other key information and review the performance of the compliance management system on a quarterly basis to ensure that the compliance management system achieves its objectives. Top management should understand the content and operation of the compliance management system and ensure that the compliance management department can manage it effectively.

The Compliance Management Department is composed of a Data Protection Committee and a Data Protection Department. Among them, the members of the data protection committee should draw on some management personnel, corporate legal personnel, and employees who have been processing data for many years to form a data committee. The function is similar to that of the headquarters, which is used to discuss the adjustment and update of internal data guide rules in the future when the law is updated, the algorithm further breaks through the reform and the actual data processing situation changes greatly, and to jointly agree on the specific determination of the content of data protection projects such as risk simulation and staff training. The data protection department is composed of company employees and is the executive department of the compliance management department. Mainly responsible for the operation of the investigation procedure, that is, the specific implementation of the data guide policy rules, and monitoring the compliance of the data methods processed by the organization's employees. In addition, a compliance report is generated every cycle for the data protection board to analyze and improve. As well as recording processed data, if any non-compliance requires immediate corrective action.

At the same time, the compliance management department also has the following characteristics: the compliance function should be independent and not affected by organizational structure or other factors. They should move freely without interference from higher management. The Compliance function has authority. The Compliance function is not a primary department that can be overruled by superiors, who can modify reports or information. Data Compliance can direct other staff as needed. The Compliance function should have a "voice" to advocate for and raise compliance issues. There must be no conflict of interest in the performance of the Compliance function.

V. Staff training, regular drills

A. Staff training

The purpose of the training program is to ensure that personnel can perform their job duties in a manner consistent with the organization's compliance culture and its commitment to compliance. The training content should include the following points: employees should master the basic knowledge of artificial intelligence in order to understand the work content; Employees need to read and memorize all the regulations in the data guide after understanding the basic knowledge of artificial intelligence. For employees with outstanding abilities and needs, they can train the operational knowledge of multiple links in the pre-training of artificial intelligence together. In order to cultivate its flexibility to adapt to the needs of different organizations and personnel, Trainees' results are subject to testing; if they pass, they become regular employees, and if they fail, they receive additional training.

B. Safety drill

In order to ensure that trainers have a real increase in data processing capabilities during the pre-training phase, while maintaining ongoing vigilance for data compliance, organizations should not rely solely on employee training testing to maintain vigilance, but should take a more proactive approach. Regular emergency drills are a key link. By simulating various common network security incidents, the reliability of

existing response mechanisms can be effectively tested, and data-related staff can have an in-depth understanding and practice of emergency procedures and solutions. Such drills help improve the team's response speed and processing efficiency when real events occur, thereby reducing the risk of data violations at the source and ensuring data security and compliance. The following is the specific operation process:

C. Safety drill

Exercise frequency: Organize a comprehensive security exercise at least once a quarter, focusing on key data processing systems and sensitive data areas. In addition, according to the industry security dynamics and internal risk assessment results, timely increase the special exercise.

Walkthrough content:

Simulate data breaches and verify the effectiveness of data classification, encryption, backup and recovery processes.

Simulate malware attacks, test anti-virus software identification and removal capabilities, and employee emergency response processes.

Simulate unauthorized access attempts to verify the reliability of access control mechanisms (such as multi-factor authentication, permission management, etc.).

Participants: Ensure that all employees involved in data processing and management are involved, especially data labelers, artificial intelligence trainers and IT security teams.

Evaluation and feedback: After the exercise, the data protection department will generate a report and submit it to the data protection committee to evaluate and analyze the exercise process, collect feedback from participants, summarize experiences and lessons, and optimize the content and process of the exercise accordingly.

Emergency plan drill

Plan formulation: according to the actual situation of the organization, formulate a detailed data security emergency plan, and clarify the emergency response process, division of responsibilities, resource allocation and other key elements.

Exercise preparation: formulate the exercise plan in advance, and specify the exercise objectives, scenes, time, place and participants. Ensure that all participants are familiar with the contents of the plan and understand their responsibilities.

Exercise implementation: conduct actual combat exercises according to the scenarios set in the plan to simulate the emergency response process in a real environment. Note the key nodes and problems during the drill.

Evaluation and improvement: after the exercise, organize an evaluation meeting to evaluate the effect of the exercise, analyze the existing problems and deficiencies, and propose improvement measures. At the same time, the plan is revised and improved according to the results of the exercise.

Fishing Penetration Test Rules Refinement

Test plan: develop a detailed phishing penetration test plan, clear test objectives, scope, methods, time nodes and expected results.

Test design: Design realistic phishing emails, links and other bait to simulate the common means of external attackers. Ensure that the test content meets the requirements of laws and regulations and does not infringe the privacy of employees.

Test execution: Perform phishing penetration tests as planned after management approval. Pay attention to control the test scope to avoid interference to normal business.

Result analysis: Collect and analyze the test results, and count the proportion, type and reason of the fishing employees. Assess the organization's level of competence in protecting against social engineering attacks.

Education and training: according to the test results, organize targeted education and training activities to improve the safety awareness and prevention ability of employees. At the same time, the test results will be incorporated into the employee performance appraisal system as one of the basis for rewards and punishments.

VI. Compliance audits, internal and external on a regular basis

A. Compliance Risk Assessment

Compliance risk assessment is fundamental to implementing a compliance management system and allocating appropriate and adequate resources and processes to manage identified compliance risks. It is a means of predicting risk, and compliance risk is generally the likelihood and consequences of non-compliance with the organization's compliance policies and obligations. Compliance risk includes inherent compliance risk and residual compliance risk. Inherent compliance risk refers to all compliance risks faced by an organization in an uncontrolled state without taking appropriate compliance risk treatment measures. Residual compliance risk refers to the compliance risk that the organization's existing compliance risk treatment measures cannot effectively control.

The department responsible for the assessment should consider the root cause, source, consequences, and likelihood of non-compliance when analyzing compliance risks. Consequences may include, for example, personal and environmental damage, economic loss, damage to reputation, administrative alteration, and civil and criminal liability.

B. Management Review

The management review should include recommendations for changes to the compliance policy and its associated objectives, systems, structures, and personnel; changes to the compliance process to ensure effective integration with operational practices and systems; identifying potential future non-compliance monitoring areas; corrective actions related to non-compliance; addressing gaps or deficiencies in the current compliance system and developing long-term continuous improvement plans; and recognizing exemplary compliance practices within the organization. The documented results of the management review and all recommendations should be provided to the governance body. The following is the specific process.

Compliance risk identification: First, the organization needs to fully identify the compliance risks it may face, including the potential risks of violating laws and regulations, industry standards, contractual obligations, and the organization's internal regulations. Risk identification should cover all business areas and management links, such as data processing, staff training, human resource management, data retention management and intellectual property management.

Risk assessment: This involves an assessment of identified compliance risks, including an analysis of the likelihood of their occurrence, potential consequences, and the probability of those occurrences. The assessment should be based on quantitative methods, such as the use of a risk matrix to prioritize risks.

Assessment of the effectiveness of existing risk management measures: Review existing risk management measures, such as policies, procedures, and controls, to determine their ability to effectively control or reduce identified compliance risks.

Risk response strategy: Based on the results of the risk assessment, a corresponding risk response strategy is formulated. This may include risk avoidance, risk transfer, risk mitigation or risk acceptance.

Fostering a culture of compliance: Promote a culture of compliance within the organization, ensure that all employees are aware of and adhere to compliance requirements, and enhance employees' awareness of compliance through training and communication.

Assessment of compliance performance: Incorporate compliance performance into the performance appraisal systems of employees and departments to ensure that compliance objectives align with the organization's overall goals.

VII. Summary

Amidst the rapid development of advanced artificial intelligence, China faces legal lags in the field of generative artificial intelligence, which presents data compliance risks. The development of artificial intelligence has created numerous data compliance issues, involving not only technical aspects but also legal and ethical considerations.

Therefore, to address these issues, including data leakage during the pre-training phase, this paper proposes the establishment of a data compliance management system. This system aims to ensure compliance in the generation, communication, and application of data by managing AI trainers. The system integrates the organization's basic structure, implementation policies, data processing processes, and compliance audit procedures to achieve the expected compliance results and take appropriate actions to prevent, detect, and respond to non-compliant data processing practices.

Based on the analysis of relevant domestic and international laws and regulations, this paper elaborates on the specific construction steps of the data compliance management system, including the formulation of data guidelines, risk assessment, event classification, judgment of the degree of harm, and the importance of ensuring compliance audit confidentiality and availability. Additionally, the article references the GDPR of the European Union and the United States' Cybersecurity Risk Management to construct a comprehensive compliance management system.

Finally, this paper hopes that this type of management system will contribute to the progress of artificial intelligence compliance. It also hopes that artificial intelligence trainers will continuously monitor relevant domestic and international laws, update their knowledge accordingly, and implement timely and appropriate contingency measures to maintain data compliance, thereby avoiding unnecessary infringement and other legal risks in the future.

References

[1] National People's Congress of the People's Republic of China. (2017). People's Republic of China Network Security Law. People's

Republic of China Central People's Government Portal. http://www.gov.cn/zhengce/2016-11/07/content_5117182.htm

[2] National People's Congress of the People's Republic of China. (2021). People's Republic of China Personal Information Protection Law. People's Republic of China Central People's Government Portal. http://www.gov.cn/zhengce/2021-08/20/content_5647.htm

[3] National People's Congress of the People's Republic of China. (2021). People's Republic of China Data Security Law. People's Republic of China Central People's Government Portal. http://www.gov.cn/zhengce/2021-06/10/content_5650.htm

[4] European Commission. (2016). General Data Protection Regulation (GDPR). Official website of the European Union. https://eur-lex.europa.eu/G3/PubDetails/lex/en/DL32016R0679.html

[5] U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. U.S. Securities and Exchange Commission official website. https://www.sec.gov/rules/final/2023/34-94267.pdf